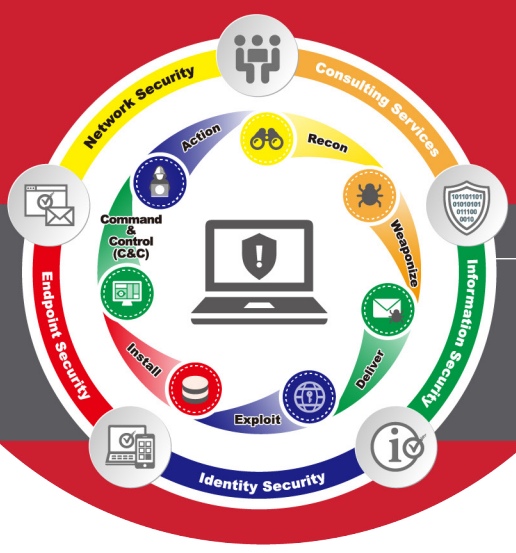

保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

名為 ApateWeb 惡意轉導向網路攻擊行動

2024 年 2 月 23 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

名為 ApateWeb 是一種惡意轉導向網路攻擊行動，會將毫無戒心的使用者帶到內藏惡意內容的網站。該行動透過欺騙性垃圾郵件或受害者瀏覽遭入侵的網站時啟動。受害者首先會收到一個 javascript 惡意有效籌載，該惡意籌載會使用一個獨特的架構對受害者進行跟蹤。

初始有效酬載收集受害者所使用的應用程式、框架、作業系統類型、版本……等指紋資訊。然後發送到攻擊者的伺服器，再利用這些資訊確定下一步的轉導向。下一步的轉導向使用隨機網域，然後再發送惡意有效酬載。最後觀察到的惡意有效酬載是潛在不受歡迎的應用程式／程式 (PUA 或 PUP)、恐嚇軟體或通知詐騙。

ApateWeb 採用多種伎倆來躲避安全研究人員的檢測和分析：

- 只有當受害者的瀏覽器檢索到帶有特定參數的網頁時，該行動才會將流量轉發到下一層。任何直接瀏覽 ApateWeb 控制網域網站的人都會被重導向到一個熱門的搜尋引擎或收到一個空頁面。這一策略有助於保護其功能變數名稱不被定期掃描網站的安全爬蟲攔截。
- 如果安全爬蟲存取了入門網頁，ApateWeb 會顯示一個錯誤頁面來隱藏自己。該行動透過檢查使用者代理來檢測爬蟲和機器人。
- ApateWeb 控制著 10,000 多個已註冊的域名，並濫用萬用字元 DNS 紀錄，這使得該行動幾乎可以透過無限多的子網域來傳播惡意內容。

賽門鐵克的網路層防護技術--入侵預防系統 (IPS) 會阻止 ApateWeb 的重導向嘗試，以防止系統受到感染／入侵。攻擊在初始階段就會被阻止，進而確保沒有惡意有效酬載被植入系統。

賽門鐵克 IPS 技術攔截到的 ApateWeb 的惡意重導向嘗試時序圖

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Web Attack: Malicious Redirection 44
- Malicious Site: Malicious Domain Request 143
- Malicious Site: Malicious Domain Request 142
- Malicious Site: Malicious Domain Request 164
- Web Attack: Malicious JavaScript Download 55

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

欲瞭解更多有關賽門鐵克端點安全入侵防護系統 (IPS) 的更多訊息，請點擊此處。
欲深入瞭解有關賽門鐵克基於雲的網路安全服務 (WebPulse) 的更多訊息，請點擊此處。

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片）軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力於賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶環境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。保安資訊連絡電話：**0800-381-500**。